A Family of Five-Weight Cyclic Codes and Their Weight Enumerators

Zhengchun Zhou, Cunsheng Ding, Jinquan Luo and Aixian Zhang

Abstract

Cyclic codes are a subclass of linear codes and have applications in consumer electronics, data storage systems, and communication systems as they have efficient encoding and decoding algorithms. In this paper, a family of p-ary cyclic codes whose duals have three zeros are proposed. The weight distribution of this family of cyclic codes is determined. It turns out that the proposed cyclic codes have five nonzero weights.

I. Introduction

An $[n,\ell,d]$ linear code over the finite field $\mathbb{F}_p$ is an ℓ-dimensional subspace of $\mathbb{F}_p^n$ with minimum (Hamming) distance d, where p is a prime. Let A_i denote the number of codewords with Hamming weight i in a code $\mathcal{C}$ of length n. The weight enumerator of $\mathcal{C}$ is defined by

$$1+A_1z+A_2z^2+\cdots+A_nz^n.$$

The sequence $(A_1,A_2,\cdots,A_n)$ is called the weight distribution of the code. Clearly, the weight distribution gives the minimum distance of the code, and thus the error correcting capability. In addition, the weight distribution of a code allows the computation of the error probability of error detection and correction with respect to some error detection and error correction algorithms [7]. Thus the study of the weight distribution of a linear code is important in both theory and applications.

An $[n,k]$ linear code $\mathcal{C}$ over $\mathbb{F}_p$ is called cyclic if $(c_0,c_1,\cdots,c_{n-1})\in\mathcal{C}$ implies $(c_{n-1},c_0,c_1,\cdots,c_{n-2})\in\mathcal{C}$. By identifying any vector $(c_0,c_1,\cdots,c_{n-1})\in\mathbb{F}_p^n$ with

$$c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}\in\mathbb{F}_p[x]/(x^n-1),$$

any code $\mathcal{C}$ of length n over $\mathbb{F}_p$ corresponds to a subset of $\mathbb{F}_p[x]/(x^n-1)$. The linear code $\mathcal{C}$ is cyclic if and only if the corresponding subset in $\mathbb{F}_p[x]/(x^n-1)$ is an ideal. It is well known that every ideal of $\mathbb{F}_p[x]/(x^n-1)$ is principal. Let $\mathcal{C}=\langle g(x)\rangle$, where $g(x)$ is monic and has the least degree. Then $g(x)$ is called the generator polynomial and $h(x)=(x^n-1)/g(x)$ is referred to as the parity-check polynomial of $\mathcal{C}$. A cyclic code is called irreducible if its parity-check polynomial is irreducible over $\mathbb{F}_p$. Otherwise, it is called reducible.

The weight distributions of both irreducible and reducible cyclic codes have been interesting subjects of study for many years and are very hard problems in general. For information on the weight distribution of irreducible cyclic codes, the reader is referred to the recent survey [2]. Information on the weight distribution of reducible cyclic codes could be found in [17], [4], [10], [11], [18], [12], [3], [15].

For the duals of the known cyclic codes whose weight distributions were established, most of them have at most two zeros (see [17], [4], [10], [11], [12], [3], [15], [16], [5], [2]), only a few of them have

Z. Zhou's research was supported by the Natural Science Foundation of China, Proj. No. 61201243. C. Ding's research was supported by The Hong Kong Research Grants Council, Proj. No. 600812. J. Luo was supported the Norwegian Research Council under Grant No. 191104/V30, the National Science Foundation (NSF) of China under Grant No. 60903036, the NSF of Jiangsu Province under Grant No. 2009182, and the Open Research Fund of the National Mobile Communications Research Laboratory, Southeast University (No. 2010D12).

Z. Zhou is with the School of Mathematics, Southwest Jiaotong University, Chengdu, 610031, China (email: zzc@home.swjtu.edu.cn).

C. Ding is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China (email: cding@ust.hk).

J. Luo is with the Department of Informatics, University of Bergen, N-5020 Bergen, Norway (email: Jinquan.Luo@ii.uib.no).

A. Zhang is with the School of Mathematical Sciences, Capital Normal University, Beijing 100048, P. R. China (email: zhangaixian1008@126.com).

three or more zeros (see [4], [10], [18], [8]). The objective of this paper is to settle the weight distribution of a family of five-weight cyclic codes whose duals have three zeros.

This paper is organized as follows. Section II defines the family of cyclic codes. Section III presents results on quadratic forms which will be needed in subsequent sections. Section IV solves the weight distribution problem for the family of cyclic codes. Section V concludes this paper and makes some comments.

II. The family of cyclic codes

In this section, we introduce the family of cyclic codes to be studied in the sequel. Before doing this, we first give some notations which will be fixed throughout the paper unless otherwise stated.

Let p be an odd prime and $q = p^m$, where m is odd and $m \geq 5$. Let $d_1 = (p^{2k}+1)/2$ and $d_2 = (p^{4k}+1)/2$, where k is any positive integer with $\gcd(m,k) = 1$. Let π be a generator of the finite field $\mathbb{F}_q$, and let $h_i(x)$ denote the minimal polynomial of π^{-i} over $\mathbb{F}_p$ for any integer i. It is easy to check that $h_1(x)$, $h_{d_1}(x)$ and $h_{d_2}(x)$ have degree m and are pairwise distinct. Define

$$h(x) = h_1(x)h_{d_1}(x)h_{d_2}(x). \tag{1}$$

Then $h(x)$ has degree $3m$ and is a factor of $x^{q-1}-1$.

Let $\mathcal{C}_{(p,m,k)}$ be the cyclic code with parity-check polynomial $h(x)$. Then $\mathcal{C}_{(p,m,k)}$ has length $q-1$ and dimension $3m$. Using the well-known Delsarte's Theorem [1], one can prove that

$$\mathcal{C}_{(p,m,k)} = \{\mathbf{c}_\Delta : \Delta = (\delta_0, \delta_1, \delta_2) \in \mathbb{F}_q^3\} \tag{2}$$

where the codeword

$$\mathbf{c}_\Delta = \left(\mathrm{Tr}(\delta_0\pi^i + \delta_1\pi^{id_1} + \delta_2\pi^{id_2})\right)_{i=0}^{q-2}$$

and Tr denotes the absolute trace from $\mathbb{F}_q$ to $\mathbb{F}_p$.

Let $h'(x) = h_1(x)h_{d_1}(x)$ and $\mathcal{C}'_{(p,m,k)}$ be the cyclic code with parity-check polynomial $h'(x)$. Then $\mathcal{C}'_{(p,m,k)}$ is a subcode of $\mathcal{C}_{(p,m,k)}$ with dimension $2m$. Trachtenberg [14] proved that $\mathcal{C}'_{(p,m,k)}$ has three nonzero weights and determined its weight distribution. The objectives of this paper are to show that $\mathcal{C}_{(p,m,k)}$ have five nonzero weights and settle the weight distribution of this class of cyclic codes $\mathcal{C}_{(p,m,k)}$.

III. Mathematical foundations

In this section, we give a brief introduction to quadratic forms over finite fields which will be useful in the sequel. Quadratic forms have been well studied (see the monograph [9] and the references therein), and have applications in sequence design ([14], [6], [13]), and coding theory ([4], [10], [11], [18]).

Definition 3.1: Let $x = \sum_{i=1}^m x_i\alpha_i$ where $x_i \in \mathbb{F}_p$ and $\{\alpha_1, \cdots, \alpha_m\}$ is a basis for $\mathbb{F}_q$ over $\mathbb{F}_p$. Then a function $Q(x)$ from $\mathbb{F}_q$ to $\mathbb{F}_p$ is a quadratic form over $\mathbb{F}_p$ if it can be represented as

$$Q(x) = Q\left(\sum_{i=1}^m x_i\alpha_i\right) = \sum_{i=1}^m \sum_{j=1}^m b_{i,j}x_ix_j$$

where $b_{i,j} \in \mathbb{F}_p$. That is, $Q(x)$ is a homogeneous polynomial of degree 2 in the ring $\mathbb{F}_p[x_1, x_2, \cdots, x_m]$.

The rank of the quadratic form $Q(x)$ is defined as the codimension of the $\mathbb{F}_p$-vector space

$$V = \{z \in \mathbb{F}_q : Q(x+z) - Q(x) - Q(z) = 0 \text{ for all } x \in \mathbb{F}_q\}.$$

That is $|V| = p^{m-r}$ where r is the rank of $Q(x)$.

In order to determine the weight distribution of the aforementioned code $\mathcal{C}_{(p,m,k)}$, we need to deal with the exponential sum of the following form:

$$S_f = \sum_{x \in \mathbb{F}_q} \zeta_p^{f(x)} \tag{3}$$

where ζ_p is a complex primitive p-th root of unity, and $f(x)$ is a function from $\mathbb{F}_q$ to $\mathbb{F}_p$ satisfying

1) $f(yx) = yf(x)$ for all $y \in \mathbb{F}_p$;
2) $Q(x) = f(x^2)$ is a quadratic form over $\mathbb{F}_p$.

Note that any nonsquare in $\mathbb{F}_p$ is also a nonsquare in $\mathbb{F}_q$ since m is odd. It is easy to verify that

$$2S_f = \sum_{x\in\mathbb{F}_q} \zeta_p^{Q(x)} + \sum_{x\in\mathbb{F}_q} \zeta_p^{\lambda Q(x)} \tag{4}$$

where λ is a fixed nonsquare in $\mathbb{F}_p$. The following result can be traced back to Trachtenberg [14] whose proof is based on (4) and the classification of quadratic forms over finite fields in odd characteristic. For more details, we refer the reader to Pages 30-36 in [14] and Lemma 4 in [13].

Lemma 3.2: Let S_f be defined by (3) and r be the rank of the quadratic form $Q(x) = f(x^2)$. Then $S_f = 0$ if r is odd, and $S_f = \pm p^{m-r/2}$ otherwise.

IV. The Weight distribution of the family of cyclic codes

In this section, we shall establish the weight distribution of the code $\mathcal{C}_{(p,m,k)}$ of (2) defined in Section II. To this end, we need a series of lemmas. Before introducing them, for any $\Delta = (\delta_0, \delta_1, \delta_2) \in \mathbb{F}_q^3$, we define

$$f_\Delta(x) = \mathrm{Tr}(\delta_0 x + \delta_1 x^{d_1} + \delta_2 x^{d_2}),\ x \in \mathbb{F}_q \tag{5}$$

and

$$S_{f_\Delta} = \sum_{x\in\mathbb{F}_q} \zeta_p^{f_\Delta(x)}. \tag{6}$$

Lemma 4.1: Let $f_\Delta(x)$ be defined by (5). Then $f_\Delta(yx) = yf_\Delta(x)$ for any $y \in \mathbb{F}_p$. And for any $\Delta \neq (0,0,0)$, the quadratic form $Q_\Delta(x) = f_\Delta(x^2)$ has rank $m-i$ for some $0 \le i \le 4$.

Proof: Recall that $d_1 = (p^{2k}+1)/2$ and $d_2 = (p^{4k}+1)/2$. Thus $y^{d_1} = y$ and $y^{d_2} = y$ for any $y \in \mathbb{F}_p$. This together with the linear properties of the trace function means that $f_\Delta(yx) = yf_\Delta(x)$ for any $y \in \mathbb{F}_p$. Clearly, $Q_\Delta(x) = f_\Delta(x^2) = \mathrm{Tr}(\delta_0 x^2 + \delta_1 x^{p^{2k}+1} + \delta_2 x^{p^{4k}+1})$ is a quadratic form over $\mathbb{F}_p$. We now calculate the rank of $Q_\Delta(x)$. Note that

$$Q_\Delta(x+z) - Q_\Delta(x) - Q_\Delta(z) = \mathrm{Tr}(zL_\Delta(x))$$

where

$$L_\Delta(x) = 2\delta_0 x + \delta_1 x^{p^{2k}} + \delta_1^{p^{-2k}} x^{p^{-2k}} + \delta_2 x^{p^{4k}} + \delta_2^{p^{-4k}} x^{p^{-4k}}.$$

We need to calculate the number of roots of the linearized polynomial $L_\Delta(x)$. Let $H_\Delta(x) = (L_\Delta(x))^{p^{4k}}$. Then

$$H_\Delta(x) = \delta_2^{p^{4k}} x^{p^{8k}} + \delta_1^{p^{4k}} x^{p^{6k}} + \delta_1^{p^{2k}} x^{p^{2k}} + 2\delta_0^{p^{4k}} x^{p^{4k}} + \delta_2 x. \tag{7}$$

Clearly, $L_\Delta(x)$ has the same number of roots in $\mathbb{F}_{p^m}$ as $H_\Delta(x)$. Fix an algebraic closure $\mathbb{F}_{p^\infty}$ of $\mathbb{F}_p$, then all roots of $H_\Delta(x)$ form a vector space over $\mathbb{F}_{p^{2k}}$ of dimension at most 4 since its degree is at most $p^{8k} = (p^{2k})^4$ for any $(\delta_0, \delta_1, \delta_2) \neq (0,0,0)$. Note that $\gcd(m, 2k) = 1$, it is straightforward (see Lemma 4, [14]) to verify that elements in $\mathbb{F}_{p^m}$ that are linearly independent over $\mathbb{F}_p$ are also linearly independent over $\mathbb{F}_{p^{2k}}$. Therefore, the roots of $H_\Delta(x)$ in $\mathbb{F}_{p^m}$ form a vector space over $\mathbb{F}_p$ of dimension at most 4. Thus the rank of $Q_\Delta(x)$ is at least $m-4$ for any $\Delta \neq (0,0,0)$. This completes the proof. ■

Lemma 4.2: Let $\mathfrak{N}_2$ denote the number of solutions $(x,y) \in \mathbb{F}_q^2$ of the following system of equations

$$\begin{cases} x + y = 0 \\ x^{d_1} + y^{d_1} = 0 \\ x^{d_2} + y^{d_2} = 0. \end{cases} \tag{8}$$

Then $\mathfrak{N}_2 = q$.

Proof: The conclusion follows directly from the observation that (x,y) is a solution of (8) if and only if $y = -x$. ■

Lemma 4.3: Let $\mathfrak{N}_3$ denote the number of solutions $(x,y,u) \in \mathbb{F}_q^3$ of the following system of equations

$$\begin{cases} x+y+u=0 \\ x^{d_1}+y^{d_1}+u^{d_1}=0 \\ x^{d_2}+y^{d_2}+u^{d_2}=0. \end{cases} \tag{9}$$

Then $\mathfrak{N}_3 = qp+q-p$.

Proof: We distinguish between the following two cases to calculate the number of solutions $(x,y,u) \in \mathbb{F}_q^3$ of (9).

Case A, when $u=0$: In this case, by Lemma 4.2, the number of solutions of (9) is equal to q.

Case B, when $u \neq 0$: In this case, for each $u \in \mathbb{F}_q^*$, the equation system (9) has the same number of solutions $(x,y) \in \mathbb{F}_q^2$ of

$$\begin{cases} 1+x+y=0 \\ 1+x^{d_1}+y^{d_1}=0 \\ 1+x^{d_2}+y^{d_2}=0 \end{cases}$$

which has the same number of solutions $x \in \mathbb{F}_q$ of

$$\begin{cases} 1+x^{d_1}=(1+x)^{d_1} \\ 1+x^{d_2}=(1+x)^{d_2}. \end{cases} \tag{10}$$

By performing square on both sides of each equation in (10), we have

$$\begin{cases} x(x^{(p^{2k}-1)/2}-1)=0 \\ x(x^{(p^{4k}-1)/2}-1)=0 \end{cases}$$

which implies that $x \in \mathbb{F}_p$ since $\gcd(m,2k)=\gcd(m,4k)=1$. Conversely, for any $x \in \mathbb{F}_p$, it is clear that x is a solution to (10) since $x^{d_i}=x$ and $(1+x)^{d_i}=1+x$ for each $i=1,2$. Thus (10) has exactly p solutions.

Summarizing the results of the two cases above, we have that $\mathfrak{N}_3 = q+(q-1)p = qp+q-p$. This completes the proof. ■

The following lemma is the key to establishing the weight distribution of the proposed code $\mathcal{C}_{(p,m,k)}$. Its proof is lengthy and is presented in Appendix I.

Lemma 4.4: Let $\mathfrak{N}_4$ denote the number of solutions $(x,y,u,v) \in \mathbb{F}_q^4$ of the following system of equations

$$\begin{cases} x+y+u+v=0 \\ x^{d_1}+y^{d_1}+u^{d_1}+v^{d_1}=0 \\ x^{d_2}+y^{d_2}+u^{d_2}+v^{d_2}=0. \end{cases} \tag{11}$$

Then $\mathfrak{N}_4 = q(qp+q-p)$.

Proof: See Appendix I. ■

Theorem 4.5: Let S_{f_Δ} be defined by (6). Then, as Δ runs through $\mathbb{F}_q^3$, the value distribution of S_{f_Δ} is given by Table I.

Proof: It is clear that $S_{f_\Delta} = p^m$ if $\Delta = (0,0,0)$. Otherwise, by Lemmas 4.1 and 3.2, we have

$$S_{f_\Delta} \in \{0, \pm p^{(m+1)/2}, \pm p^{(m+3)/2}\}.$$

To determine the distribution of these values, we define

$$\begin{aligned} n_{1,i} &= \#\{\Delta \in \mathbb{F}_q^3 \setminus \{(0,0,0)\} : \ S_{f_\Delta} = (-1)^i p^{(m+1)/2}\}, \\ n_{2,i} &= \#\{\Delta \in \mathbb{F}_q^3 \setminus \{(0,0,0)\} : \ S_{f_\Delta} = (-1)^i p^{(m+3)/2}\} \end{aligned}$$

TABLE I
VALUE DISTRIBUTION OF S_{f_Δ}

Value	Frequency
p^m	1
0	$(p^m-1)(p^{2m}-p^{2m-1}+p^{2m-4}+p^m-p^{m-1}-p^{m-3}+1)$
$p^{(m+1)/2}$	$\frac{(p^{m+1}+p^{(m+3)/2})(p^{2m}-p^{2m-2}-p^{2m-3}+p^{m-2}+p^{m-3}-1)}{2(p^2-1)}$
$-p^{(m+1)/2}$	$\frac{(p^{m+1}-p^{(m+3)/2})(p^{2m}-p^{2m-2}-p^{2m-3}+p^{m-2}+p^{m-3}-1)}{2(p^2-1)}$
$p^{(m+3)/2}$	$\frac{(p^{m-3}+p^{(m-3)/2})(p^{m-1}-1)(p^m-1)}{2(p^2-1)}$
$-p^{(m+3)/2}$	$\frac{(p^{m-3}-p^{(m-3)/2}(p^{m-1}-1)(p^m-1)}{2(p^2-1)}$

where $i=0,1$. Then the value distribution of S_{f_Δ} is as follows

$$\begin{array}{lll} p^m & \text{occurring} & 1 \text{ time} \\ p^{(m+1)/2} & \text{occurring} & n_{1,0} \text{ times} \\ -p^{(m+1)/2} & \text{occurring} & n_{1,1} \text{ times} \\ p^{(m+3)/2} & \text{occurring} & n_{2,0} \text{ times} \\ -p^{(m+3)/2} & \text{occurring} & n_{2,1} \text{ times} \\ 0 & \text{occurring} & p^{3m}-1-n_1-n_2 \text{ times.} \end{array} \tag{12}$$

By (12), we immediately have

$$\begin{cases} \sum_{\Delta\in\mathbb{F}_q^3} S_{f_\Delta} &= p^m+(n_{1,0}-n_{1,1})p^{(m+1)/2}+(n_{2,0}-n_{2,1})p^{(m+3)/2} \\ \sum_{\Delta\in\mathbb{F}_q^3} S_{f_\Delta}^2 &= p^{2m}+(n_{1,0}+n_{1,1})p^{m+1}+(n_{2,0}+n_{2,1})p^{m+3} \\ \sum_{\Delta\in\mathbb{F}_q^3} S_{f_\Delta}^3 &= p^{3m}+(n_{1,0}-n_{1,1})p^{(3m+3)/2}+(n_{2,0}-n_{2,1})p^{(3m+9)/2} \\ \sum_{\Delta\in\mathbb{F}_q^3} S_{f_\Delta}^4 &= p^{4m}+(n_{1,0}+n_{1,1})p^{2m+2}+(n_{2,0}+n_{2,1})p^{2m+6}. \end{cases} \tag{13}$$

On the other hand, applying Lemmas 4.2, 4.3 and 4.4, we have

$$\begin{array}{lll} \sum_{\Delta\in\mathbb{F}_q^3} S_{f_\Delta} &= p^{3m} \\ \sum_{\Delta\in\mathbb{F}_q^3} S_{f_\Delta}^2 &= p^{4m} \\ \sum_{\Delta\in\mathbb{F}_q^3} S_{f_\Delta}^3 &= p^{3m}(p^{m+1}+p^m-p) \\ \sum_{\Delta\in\mathbb{F}_q^3} S_{f_\Delta}^4 &= p^{4m}(p^{m+1}+p^m-p). \end{array} \tag{14}$$

Combining Equations (13) and (14) gives

$$n_{1,0}=\frac{(p^{m+1}+p^{(m+3)/2})(p^{2m}-p^{2m-2}-p^{2m-3}+p^{m-2}+p^{m-3}-1)}{2(p^2-1)},$$

$$n_{1,1}=\frac{(p^{m+1}-p^{(m+3)/2})(p^{2m}-p^{2m-2}-p^{2m-3}+p^{m-2}+p^{m-3}-1)}{2(p^2-1)},$$

$$n_{2,0}=\frac{(p^{m-3}+p^{(m-3)/2})(p^{m-1}-1)(p^m-1)}{2(p^2-1)},$$

$$n_{2,1}=\frac{(p^{m-3}-p^{(m-3)/2})(p^{m-1}-1)(p^m-1)}{2(p^2-1)}.$$

TABLE II
WEIGHT DISTRIBUTION OF THE CODE $\mathcal{C}_{(p,m,k)}$ IN THEOREM 4.6

Hamming Weight	Frequency
0	1
$(p-1)p^{m-1}$	$(p^m-1)(p^{2m}-p^{2m-1}+p^{2m-4}+p^m-p^{m-1}-p^{m-3}+1)$
$(p-1)(p^{m-1}-p^{(m-1)/2})$	$\frac{(p^{m+1}+p^{(m+3)/2})(p^{2m}-p^{2m-2}-p^{2m-3}+p^{m-2}+p^{m-3}-1)}{2(p^2-1)}$
$(p-1)(p^{m-1}+p^{(m-1)/2})$	$\frac{(p^{m+1}-p^{(m+3)/2})(p^{2m}-p^{2m-2}-p^{2m-3}+p^{m-2}+p^{m-3}-1)}{2(p^2-1)}$
$(p-1)(p^{m-1}-p^{(m+1)/2})$	$\frac{(p^{m-3}+p^{(m-3)/2})(p^{m-1}-1)(p^m-1)}{2(p^2-1)}$
$(p-1)(p^{m-1}+p^{(m+1)/2})$	$\frac{(p^{m-3}-p^{(m-3)/2})(p^{m-1}-1)(p^m-1)}{2(p^2-1)}$

The value distribution of S_{f_Δ} depicted in Table I then follows from the values of $n_{1,0}, n_{1,1}, n_{2,0}$ and $n_{2,1}$, and the analysis above. ■

The following is the main result of the paper.

Theorem 4.6: Let $\mathcal{C}_{(p,m,k)}$ be the code in (2). Then $\mathcal{C}_{(p,m,k)}$ is a cyclic code over $\mathbb{F}_p$ with parameters

$$[p^m-1, 3m, (p-1)(p^{m-1}-p^{(m+1)/2})].$$

Furthermore, the weight distribution of $\mathcal{C}_{(p,m,k)}$ is given by Table II.

Proof: The length and dimension of the code follow directly from the definition of $\mathcal{C}_{(p,m,k)}$. We only need to determine its minimal weight and weight distribution. In terms of exponential sums, the weight of the codeword $\mathbf{c}_\Delta$ in $\mathcal{C}_{(p,m,k)}$ is given by

$$\begin{aligned}
\mathrm{WT}(\mathbf{c}_\Delta) &= \#\{x \in \mathbb{F}_q^* : \quad \mathrm{Tr}(\delta_0 x + \delta_1 x^{d_1} + \delta_2 x^{d_2}) \neq 0\} \\
&= q-1-\#\{x \in \mathbb{F}_q^* : \quad \mathrm{Tr}(\delta_0 x + \delta_1 x^{d_1} + \delta_2 x^{d_2}) = 0\} \\
&= q-1-\frac{1}{p}\sum_{x\in\mathbb{F}_q^*}\sum_{y\in\mathbb{F}_p} \zeta_p^{y\mathrm{Tr}(\delta_0 x+\delta_1 x^{d_1}+\delta_2 x^{d_2})} \\
&= p^m - p^{m-1} - \frac{1}{p}\sum_{y\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}(\delta_0 yx+\delta_1 yx^{d_1}+\delta_2 yx^{d_2})} \\
&= (p-1)p^{m-1} - \frac{1}{p}\sum_{y\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}(\delta_0 yx+\delta_1 (yx)^{d_1}+\delta_2 (yx)^{d_2})} \\
&= (p-1)p^{m-1} - \frac{1}{p}\sum_{y\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}(\delta_0 x+\delta_1 x^{d_1}+\delta_2 x^{d_2})} \\
&= (p-1)p^{m-1} - \frac{p-1}{p} S_{f_\Delta} \qquad (15)
\end{aligned}$$

where S_{f_Δ} is given by (6) and in the fifth identity we used the fact that $y^{d_i} = y$ for any $y \in \mathbb{F}_p$. The minimal weight and weight distribution of $\mathcal{C}_{(p,m,k)}$ then follow from (15) and the value distribution of the exponential sum S_{f_Δ} depicted in Table I. ■

Example 4.7: Let $p=3$, $m=5$ and $k=1$. Then the code $\mathcal{C}_{(p,m,k)}$ is a $[242, 15, 108]$ code over $\mathbb{F}_3$ with the weight enumerator

$$1 + 14520z^{108} + 2548260z^{144} + 9740258z^{162} + 2038608z^{180} + 7260z^{216}$$

which confirms the weight distribution in Table II.

TABLE III
WEIGHT DISTRIBUTION OF THE CODE $\mathcal{C}_{(p,m,k)}$ IN THEOREM 5.1

Hamming Weight	Frequency
0	1
$(p-1)p^{m-1}$	$(p^m-1)(p^{2m}-p^{2m-e}+p^{2m-4e}+p^m-p^{m-e}-p^{m-3e}+1)$
$(p-1)(p^{m-1}-p^{(m+e-2)/2})$	$\frac{(p^{m+e}+p^{(m+3e)/2})(p^{2m}-p^{2m-2e}-p^{2m-3e}+p^{m-2e}+p^{m-3e}-1)}{2(p^{2e}-1)}$
$(p-1)(p^{m-1}+p^{(m+e-2)/2})$	$\frac{(p^{m+e}-p^{(m+3e)/2})(p^{2m}-p^{2m-2e}-p^{2m-3e}+p^{m-2e}+p^{m-3e}-1)}{2(p^{2e}-1)}$
$(p-1)(p^{m-1}-p^{(m+3e-2)/2})$	$\frac{(p^{m-3e}+p^{(m-3e)/2})(p^{m-e}-1)(p^m-1)}{2(p^{2e}-1)}$
$(p-1)(p^{m-1}+p^{(m+3e-2)/2})$	$\frac{(p^{m-3e}-p^{(m-3e)/2})(p^{m-e}-1)(p^m-1)}{2(p^{2e}-1)}$

Example 4.8: Let $p=3$, $m=7$ and $k=2$. Then the code $\mathcal{C}_{(p,m,k)}$ is a $[2186,21,1296]$ code over $\mathbb{F}_3$ with the weight enumerator

$$1+8951670z^{1296}+1732767876z^{1404}+7102473578z^{1458}+1608998742z^{1512}+7161336z^{1620}$$

which confirms the weight distribution in Table II.

Example 4.9: Let $p=5$, $m=5$ and $k=1$. Then the code $\mathcal{C}_{(p,m,k)}$ is a $[3124,15,2000]$ code over $\mathbb{F}_3$ with the weight enumerator

$$1+1218360z^{2000}+3147430000z^{2400}+24462797524z^{2500}+2905320000z^{2600}+812240z^{3000}$$

which confirms the weight distribution in Table II.

V. SUMMARY AND CONCLUDING REMARKS

In this paper, we studied a family of five-weight cyclic codes. The duals of the cyclic codes have three zeros. The weight distribution of this family of cyclic codes is completely determined.

Finally we mention that the weight distribution of $\mathcal{C}_{(p,m,k)}$ can also be settled in a more general case where $m/\gcd(m,k)$ is odd. In what follows we only report the conclusion. The proof is similar to that of Theorem 4.6.

Theorem 5.1: Let $\gcd(m,k)=e$, m/e be odd, and $m/e\geq 5$. Let $\mathcal{C}_{(p,m,k)}$ be the code in (2). Then $\mathcal{C}_{(p,m,k)}$ is a cyclic code over $\mathbb{F}_p$ with parameters

$$[p^m-1, 3m, (p-1)(p^{m-1}-p^{(m+3e-2)/2})].$$

Furthermore, the weight distribution of $\mathcal{C}_{(p,m,k)}$ is given by Table III.

APPENDIX I

Proof of Lemma 4.4:

For any $(\overline{a},\overline{b},\overline{c})\in\mathbb{F}_q^3$, let $\overline{N}_{(\overline{a},\overline{b},\overline{c})}$ denote the number of solutions $(x,y,u,v)\in\mathbb{F}_q^4$ of the following system of equations

$$\begin{cases} x+y=\overline{a} \\ x^{d_1}+y^{d_1}=\overline{b} \\ x^{d_2}+y^{d_2}=\overline{c} \\ u+v=-\overline{a} \\ u^{d_1}+v^{d_1}=-\overline{b} \\ u^{d_2}+v^{d_2}=-\overline{c}. \end{cases} \tag{16}$$

It is then obvious that

$$\mathfrak{N}_4 = \sum_{(\overline{a},\overline{b},\overline{c})\in\mathbb{F}_q^3} \overline{N}_{(\overline{a},\overline{b},\overline{c})}.$$

For any $(\overline{a},\overline{b},\overline{c}) \in \mathbb{F}_q^3$, let $\hat{N}_{(\overline{a},\overline{b},\overline{c})}$ denote the number of solutions $(x,y) \in \mathbb{F}_q^2$ of the following system of equations

$$\begin{cases} x+y = \overline{a} \\ x^{d_1}+y^{d_1} = \overline{b} \\ x^{d_2}+y^{d_2} = \overline{c}. \end{cases} \tag{17}$$

Since d_1 and d_2 are odd, $\overline{N}_{(\overline{a},\overline{b},\overline{c})} = \left(\hat{N}_{(\overline{a},\overline{b},\overline{c})}\right)^2$, we have

$$\mathfrak{N}_4 = \sum_{(\overline{a},\overline{b},\overline{c})\in\mathbb{F}_q^3} \left(\hat{N}_{(\overline{a},\overline{b},\overline{c})}\right)^2. \tag{18}$$

We distinguish among the following three cases to calculate $\hat{N}_{(\overline{a},\overline{b},\overline{c})}$.

Case A, when $\overline{a} = \overline{b} = \overline{c} = 0$: In this case, $\hat{N}_{(0,0,0)} = q$ since (x,y) is a solution of (17) if and only if $y = -x$. Thus $(\hat{N}_{(0,0,0)})^2 = q^2$.

Case B, when $\overline{a} \neq 0$, and ($\overline{b} = 0$ or $\overline{c} = 0$): In this case, it is clear that $\hat{N}_{(\overline{a},\overline{b},\overline{c})} = 0$.

Case C, when $\overline{a} \neq 0$, $\overline{b} \neq 0$ and $\overline{c} \neq 0$. In this case, for any given $\overline{a} \neq 0$, Equation System (17) has the same number of solutions as

$$\begin{cases} x+y = 1 \\ x^{d_1}+y^{d_1} = b \\ x^{d_2}+y^{d_2} = c \end{cases} \tag{19}$$

where $b = \overline{b}/\overline{a}^{d_1}$ and $c = \overline{c}/\overline{a}^{d_2}$. Clearly, (b,c) runs over $\mathbb{F}_q^* \times \mathbb{F}_q^*$ as $(\overline{b},\overline{c})$ does. By Lemma 5.2, we have

$$\sum_{(\overline{a},\overline{b},\overline{c})\in(\mathbb{F}_q^*)^3} \left(\hat{N}_{(\overline{a},\overline{b},\overline{c})}\right)^2 = (q-1)\left[p^2 + (p+1)^2\frac{q-p}{2(p+1)} + (p-1)^2\frac{q-p}{2(p-1)}\right] = q(qp-p).$$

Summarizing all the cases above, we have

$$\mathfrak{N}_4 = q^2 + q(qp-p) = q(qp+q-p).$$

This completes the proof.

Lemma 5.2: Let $\mathsf{N}_{(b,c)}$ denote the number of solutions $(x,y) \in \mathbb{F}_q^2$ of (19), where $(b,c) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$. Then we have the following conclusions.

B1 $\mathsf{N}_{(1,1)} = p$.

B2 When (b,c) runs over $\mathbb{F}_q^* \times \mathbb{F}_q^* \setminus \{(1,1)\}$,

$$\mathsf{N}_{(b,c)} = \begin{cases} p+1 & \text{for } \frac{q-p}{2(p+1)} \text{ times} \\ p-1 & \text{for } \frac{q-p}{2(p-1)} \text{ times} \\ 0 & \text{for the rest.} \end{cases}$$

The proof of Lemma 5.2 is lengthy and technical. We first prove some auxiliary results.

AUXILIARY RESULTS FOR PROVING LEMMA 5.2

We prove Lemma 5.2 only for the case that $p \equiv 3 \pmod 4$. The proof for the case $p \equiv 1 \pmod 4$ is similar and omitted. Hence we assume that $p \equiv 3 \pmod 4$ from now on.

A. Case 1

In (19) we substitute (x,y) with $(x_1^2,-y_1^2)$ and obtain the following system of equations

$$\begin{cases} x_1^2-y_1^2=1 \\ x_1^{2d_1}-y_1^{2d_1}=b \\ x_1^{2d_2}-y_1^{2d_2}=c \end{cases} \tag{20}$$

where $b,c\in\mathbb{F}_q^*$. Our task is to compute the number $\mathtt{N}_{(b,c)}$ of solutions $(x_1,y_1)\in\mathbb{F}_q^2$ of (20). To this end, we first compute the number $\mathtt{N}_b$ of solutions $(x_1,y_1)\in\mathbb{F}_q^2$ of the following system of equations

$$\begin{cases} x_1^2-y_1^2=1 \\ x_1^{2d_1}-y_1^{2d_1}=b \end{cases} \tag{21}$$

where $b\in\mathbb{F}_q^*$.

Lemma 5.3: Let symbols and notations be the same as before. As for Equation (21), we have

$$\mathtt{N}_b=\begin{cases} p-1 & \text{if } b=1 \\ 2(p-1) & \text{for } \frac{q-p}{2(p-1)} \text{ elements } b\neq 1 \\ 0 & \text{for the rest } b\neq 1. \end{cases}$$

Proof: Let (x_1,y_1) be a solution of the first equation in (21). It is clear that $x_1\neq y_1$. Let $\theta=x_1-y_1$. It then follows that $\theta\in\mathbb{F}_q^*$ and

$$x_1=\frac{\theta+\theta^{-1}}{2},\ y_1=\frac{\theta^{-1}-\theta}{2}. \tag{22}$$

Thus (x_1,y_1) is uniquely determined by θ. Substituting (22) into the second equation of (21), we obtain

$$\theta^{p^{2k}-1}+\theta^{1-p^{2k}}=2b. \tag{23}$$

Let $w=\theta^{p^{2k}-1}$. Then (23) is equivalent to

$$w^2-2bw+1=0. \tag{24}$$

If (24) has no solution, i.e., b^2-1 is not a square in $\mathbb{F}_q^*$, then $\mathtt{N}_b=0$. Otherwise, suppose that w_1 and $w_2=w_1^{-1}$ are two solutions of (24). We then have

$$\theta^{p^{2k}-1}=w_1 \tag{25}$$

or

$$\theta^{p^{2k}-1}=w_1^{-1}. \tag{26}$$

Clearly, (25) and (26) have the same number of solutions $\theta\in\mathbb{F}_q$. Note that $\gcd(p^{2k}-1,q-1)=p-1$. Thus both (25) and (26) have no solution or exactly $p-1$ solutions. If $w_1=w_1^{-1}$, then $w_1=\pm1$ and $b=\pm1$. However -1 is not a square, thus, $w_1=1$ and $b=1$. In this case, (25) and (26) become the same equation and have $p-1$ solutions. If $w_1\neq w_1^{-1}$, then (25) and (26) have distinct solutions.

Based on above analysis, we conclude

$$\mathtt{N}_1=p-1 \text{ and } \mathtt{N}_b=0 \text{ or } 2(p-1) \text{ for } b\neq 1.$$

Define

$$T=\#\{b\in\mathbb{F}_q : N_b=2(p-1)\}.$$

Note that the first equation in (21) has $q-1$ solutions in $\mathbb{F}_q$ thanks to Lemma 6.24 in [9]. When (x,y) runs through all these solutions, the second equation in (21) will give a $2(p-1)$-to-1 correspondence

$$(x,y)\mapsto b=x^{p^{2k}+1}-y^{p^{2k}+1}$$

if $N_b = 2(p-1)$. Therefore

$$(p-1)+2(p-1)T = q-1$$

which leads to

$$T = \frac{q-p}{2(p-1)}.$$

This completes the proof. ■

Lemma 5.4: Let symbols and notations be the same as before. As for Equation System (20), we have

$$\mathtt{N}_{(b,c)} = \begin{cases} p-1 & \text{if } (b,c) = (1,1) \\ 2(p-1) & \text{for } \frac{q-p}{2(p-1)} \text{ pairs } (b,c) \neq (1,1) \\ 0 & \text{for the rest pairs} (b,c) \in (\mathbb{F}_q^*)^2 \setminus \{(1,1)\}. \end{cases}$$

Proof: Let (x_1, y_1) be any solution of (20). Let $\theta = x_1 - y_1$. It then follows from the first equation in (21) that

$$x_1 = \frac{\theta + \theta^{-1}}{2},\ y_1 = \frac{\theta^{-1} - \theta}{2}. \tag{27}$$

Using the second and third equations in (20), we obtain

$$\begin{cases} b = \frac{1}{2}\left(\theta^{p^{2k}-1} + \theta^{1-p^{2k}}\right) \\ c = \frac{1}{2}\left(\theta^{p^{4k}-1} + \theta^{1-p^{4k}}\right). \end{cases}$$

Let $w = \theta^{p^{2k}-1}$ and

$$\begin{cases} \tilde{b} = \left(\theta^{p^{2k}-1} + \theta^{1-p^{2k}}\right) = w + w^{-1} \\ \tilde{c} = \left(\theta^{p^{4k}-1} + \theta^{1-p^{4k}}\right) = w^{p^{2k}+1} + (w^{-1})^{p^{2k}+1}. \end{cases} \tag{28}$$

Then $w^2 - \tilde{b}w + 1 = 0$ and

$$w = \frac{\tilde{b}}{2} \pm \sqrt{\left(\frac{\tilde{b}}{2}\right)^2 - 1}.$$

It follows from the first equation in (28) that

$$\tilde{b}^{p^{2k}} = w^{p^{2k}} + (w^{-1})^{p^{2k}}. \tag{29}$$

Combining the first equation in (28) and (29), we obtain

$$\tilde{b}^{p^{2k}+1} = \tilde{c} + w^{p^{2k}-1} + (w^{-1})^{p^{2k}-1}.$$

Whence,

$$\tilde{c} = \tilde{b}^{p^{2k}+1} - \left(w^{p^{2k}-1} + (w^{-1})^{p^{2k}-1}\right). \tag{30}$$

Note that

$$w = \frac{\tilde{b}}{2} \pm \sqrt{\left(\frac{\tilde{b}}{2}\right)^2 - 1}$$

if and only if

$$w^{-1} = \frac{\tilde{b}}{2} \mp \sqrt{\left(\frac{\tilde{b}}{2}\right)^2 - 1}.$$

By (30), $\tilde{c}$ is uniquely determined by $\tilde{b}$. Therefore, c is uniquely determined by b.

In addition, it is easily seen that $\tilde{c}=2$ if and only if $\tilde{b}=2$.

Hence the number of solutions of (20) is the same as that of (21). The desired conclusions then follow from Lemma 5.3. ■

Lemma 5.5: Let $\mathtt{M}_{(b,c)}$ denote the number of solutions (x,y) of (19) such that x is a square and y is a nonquare or $y=0$. Then

$$\mathtt{M}_{(b,c)}=\begin{cases}\frac{p+1}{4} & \text{if } (b,c)=(1,1)\\ \frac{p-1}{2} & \text{for } \frac{q-p}{2(p-1)} \text{ pairs } (b,c)\neq(1,1)\\ 0 & \text{for the rest pairs} (b,c)\in(\mathbb{F}_q^*)^2\setminus\{(1,1)\}.\end{cases}$$

Proof: Consider now the solutions of (20). If (x_1,y_1) is a solution of (20), so are $(-x_1,y_1)$, $(x_1,-y_1)$ and $(-x_1,-y_1)$. If $y_1\neq 0$, they are indeed four different solutions of (20), but give only one solution of (19).

Since -1 is a quadratic nonresidue in $\mathbb{F}_q$, $x_1\neq 0$. However, it is possible that $y_1=0$. If $y_1=0$, then $(b,c)=(1,1)$. In this case, we have two special solutions $(\pm 1,0)$ of (20). They give only one solution of (19).

It then follows from Lemma 5.4 that

$$\mathtt{M}_{(1,1)}=\frac{\mathtt{N}_{(1,1)}-2}{4}+1=\frac{p-3}{4}+1=\frac{p+1}{4}$$

and

$$\begin{aligned}\mathtt{M}_{(b,c)} &= \frac{\mathtt{N}_{(b,c)}}{4}\\ &= \begin{cases}\frac{p-1}{2} & \text{for } \frac{q-p}{2(p-1)} \text{ pairs } (b,c)\neq(1,1)\\ 0 & \text{for the rest pairs} (b,c)\in(\mathbb{F}_q^*)^2\setminus\{(1,1)\}.\end{cases}\end{aligned}$$

The proof is then completed. ■

B. Case 2

Lemma 5.6: Let $\mathtt{M}_{(b,c)}$ denote the number of solutions (x,y) of (19) such that y is a square and x is a nonsquare or $x=0$. Then

$$\mathtt{M}_{(b,c)}=\begin{cases}\frac{p+1}{4} & \text{if } (b,c)=(1,1)\\ \frac{p-1}{2} & \text{for } \frac{q-p}{2(p-1)} \text{ pairs } (b,c)\neq(1,1)\\ 0 & \text{for the rest pairs} (b,c)\in(\mathbb{F}_q^*)^2\setminus\{(1,1)\}.\end{cases}$$

This case is symmetric to Case 1. Hence the proof of this lemma is similar to that of Lemma 5.5 and is omitted.

C. Case 3

In (19) we substitute (x,y) with (x_1^2,y_1^2) and obtain the following system of equations

$$\begin{cases}x_1^2+y_1^2=1\\ x_1^{2d_1}+y_1^{2d_1}=b\\ x_1^{2d_2}+y_1^{2d_2}=c\end{cases}\tag{31}$$

where $b,c\in\mathbb{F}_q^*$. Our task is to compute the number $N_{(b,c)}$ of solutions $(x_1,y_1)\in\mathbb{F}_q^2$ of (31). To this end, we first compute the number $\mathtt{N}_b$ of solutions $(x_1,y_1)\in\mathbb{F}_q^2$ of the following system of equations

$$\begin{cases}x^2+y^2=1\\ x^{p^{2k}+1}+y^{p^{2k}+1}=b\end{cases}\tag{32}$$

where $b \in \mathbb{F}_q^*$.

Lemma 5.7: Let symbols and notations be the same as before. As for Equation (32), we have

$$N_b = \begin{cases} p+1 & \text{if } b = 1 \\ 2(p+1) & \text{for } \frac{q-p}{2(p+1)} \text{ elements } b \neq 1 \\ 0 & \text{for the rest } b \neq 1. \end{cases}$$

Proof: Choose $t \in \mathbb{F}_{p^2}$ such that $t^2 = -1$. From

$$x^2 + y^2 = 1 \tag{33}$$

we can assume

$$x = \frac{\theta + \theta^{-1}}{2}, \qquad y = \frac{t(\theta - \theta^{-1})}{2} \tag{34}$$

with $\theta \in \mathbb{F}_{q^2}^*$. It is easy to see that all the solutions $(x,y) \in \mathbb{F}_q^2$ of (33) can be expressed as in (34) with a unique $\theta \in \mathbb{F}_{q^2}^*$. Substituting (34) into

$$x^{p^{2k}+1} + y^{p^{2k}+1} = b, \tag{35}$$

we obtain

$$\theta^{p^{2k}-1} + \theta^{1-p^{2k}} = 2b. \tag{36}$$

Denote by $w = \theta^{p^{2k}-1}$. Then (36) is equivalent to

$$w^2 - 2bw + 1 = 0. \tag{37}$$

Let w_1 and $w_2 = w_1^{-1}$ be two solutions of (37). Then we have $w_1 \in \mathbb{F}_{q^2}^*$.

From (34) and $x \in \mathbb{F}_q$ we have

$$\theta + \theta^{-1} = (\theta + \theta^{-1})^q = \theta^q + \theta^{-q}$$

which implies

$$\theta^{q+1} = 1 \text{ or } \theta^{q-1} = 1.$$

- If $\theta^{q+1} = 1$, then $y^q = \frac{t^q(\theta^q - \theta^{-q})}{2} = \frac{t(\theta - \theta^{-1})}{2} = y$ since $t^q = -t$. It follows that $y \in \mathbb{F}_q$. For a fixed b, recall that w_1 and $w_2 = w_1^{-1}$ are two solutions of (37). Then we have

  $$\theta^{p^{2k}-1} = w_1, \quad \theta^{q+1} = 1 \tag{38}$$

  or

  $$\theta^{p^{2k}-1} = w_1^{-1}, \quad \theta^{q+1} = 1. \tag{39}$$

  If θ_1 and θ_2 are two solutions of (38), then $(\theta_1/\theta_2)^{p^{2k}-1} = (\theta_1/\theta_2)^{q+1} = 1$ which is equivalent to $(\theta_1/\theta_2)^{p+1} = 1$. As a consequence, if (38) has solutions, then it has exactly $p+1$ solutions.
  If $w_1 = w_1^{-1}$, then (39) is the same with (38) and apparently it gives no more solutions. In this case $w_1 = \pm 1$ and $b = \pm 1$. But $b = -1$ can be excluded since, otherwise, $w_1 = -1$, then $\theta^{p^{2k}-1} = -1$ which contradicts to $\theta \in \mathbb{F}_{p^{2m}}$. The remaining case is $b = 1$ which corresponds to $w_1 = 1$. In this case we have $p+1$ solutions of θ which gives exactly the same number of solutions of (32).
  If $w_1 \neq w_1^{-1}$, then (39) has the same number of solutions as (38) and moreover, their solutions are distinct. Therefore (38) and (39) both have $p+1$ solutions or no solutions in $\mathbb{F}_{q^2}$.
- If $\theta^{q-1} = 1$ and $\theta^{q+1} \neq 1$, then $\theta \in \mathbb{F}_q^*$. Note that $t \notin \mathbb{F}_q^*$, $y = \frac{t(\theta - \theta^{-1})}{2}$ is not in $\mathbb{F}_q^*$ except for $\theta = \theta^{-1} = \pm 1$. But the exception case will not occur since $\theta^{q+1} \neq 1$.

Summarizing up, we conclude

$$N_1 = p+1 \text{ and } N_b = 0 \text{ or } 2(p+1) \text{ for } b \neq 1.$$

Define

$$T = \#\{b \in \mathbb{F}_q : N_b = 2(p+1)\}.$$

Note that (33) has $q+1$ solutions in $\mathbb{F}_q$ thanks to Lemma 6.24 in [9]. When (x,y) runs through all these solutions, the equation (35) will give a $2(p+1)$-to-1 correspondence

$$(x,y) \mapsto b = x^{p^{2k}+1} + y^{p^{2k}+1}$$

if $N_b = 2(p+1)$. Therefore

$$(p+1) + 2(p+1)T = q+1$$

which implies

$$T = \frac{q-p}{2(p+1)}.$$

The proof is now finished. ■

Lemma 5.8: Let symbols and notations be the same as before. As for Equation System (31), we have

$$N_{(b,c)} = \begin{cases} p+1 & \text{if } (b,c) = (1,1) \\ 2(p+1) & \text{for } \frac{q-p}{2(p+1)} \text{ pairs } (b,c) \neq (1,1) \\ 0 & \text{for the rest } (b,c) \neq (1,1). \end{cases}$$

Proof: The proof of this lemma is similar to that of Lemma 5.4 and is derived from Lemma 5.7. The details of the proof is omitted here. ■

Lemma 5.9: Let $M_{(b,c)}$ denote the number of solutions (x,y) of (19) such that both x and y are squares. Then

$$M_{(b,c)} = \begin{cases} \frac{p+5}{4} & \text{if } (b,c) = (1,1) \\ \frac{p+1}{2} & \text{for } \frac{q-p}{2(p+1)} \text{ pairs } (b,c) \neq (1,1) \\ 0 & \text{for the rest pairs} (b,c) \in (\mathbb{F}_q^*)^2 \setminus \{(1,1)\}. \end{cases}$$

Proof: Consider now the solutions of (31). If (x_1,y_1) is a solution of (31), so are $(-x_1,y_1)$, $(x_1,-y_1)$ and $(-x_1,-y_1)$. If $x_1y_1 \neq 0$, they are indeed four different solutions of (31), but give only one solution of (19).

However, it is possible that $x_1y_1 = 0$. If $(b,c) = (1,1)$, Equation (31) has four special solutions $(\pm 1, 0)$ and $(0, \pm 1)$. They give only two solutions of (19). It then follows from Lemma 5.8 that

$$M_{(1,1)} = \frac{N_{(1,1)} - 4}{4} + 2 = \frac{p+5}{4}.$$

If $(b,c) \neq (1,1)$, then the four distinct solutions $(\pm x_1, \pm y_1)$ give only one solution of (19). In this case, it then follows from Lemma 5.8 that

$$\begin{aligned} M_{(b,c)} &= \frac{N_{(b,c)}}{4} \\ &= \begin{cases} \frac{p+1}{2} & \text{for } \frac{q-p}{2(p+1)} \text{ pairs } (b,c) \neq (1,1) \\ 0 & \text{for the rest pairs} (b,c) \in (\mathbb{F}_q^*)^2 \setminus \{(1,1)\}. \end{cases} \end{aligned}$$

The proof is then completed. ■

D. Case 4

Lemma 5.10: Let $M_{(b,c)}$ denote the number of solutions (x,y) of (19) such that both x and y are either nonsquares or zero. Then

$$M_{(b,c)} = \begin{cases} \frac{p-3}{4} & \text{if } (b,c) = (1,1) \\ \frac{p+1}{2} & \text{for } \frac{q-p}{2(p+1)} \text{ pairs } (b,c) \neq (1,1) \\ 0 & \text{for the rest pairs} (b,c) \in (\mathbb{F}_q^*)^2 \setminus \{(1,1)\}. \end{cases}$$

Proof: The proof of this lemma is similar to that of Lemma 5.9 and is omitted here. ■

THE PROOF OF LEMMA 5.2

Note that the solutions $(1,0)$ and $(0,1)$ of (19) are counted more than once in Cases 1, 2, 3 and 4. By analyzing the proofs of Lemmas 5.5, 5.6, 5.9 and 5.10, we have

$$\mathtt{N}_{(1,1)} = \frac{p-3}{4} + \frac{p-3}{4} + \frac{p+1}{4} + \frac{p-3}{4} + 2 = p.$$

When $(b,c) \neq (1,1)$, $\mathtt{N}_{(\mathtt{b},\mathtt{c})}$ is the sum of the solutions given in Lemmas 5.5, 5.6, 5.9 and 5.10. This completes the proof.

REFERENCES

[1] P. Delsarte, "On subfield subcodes of modified Reed-Solomon codes," *IEEE Trans. Inform. Theory,* vol. IT-21, no. 5, pp. 575–576, Sep. 1975.

[2] C. Ding and J. Yang, "Hamming weights in irreducible cyclic codes," *Discrete Mathematics*, vol. 313, no. 4, pp. 434–446, Feb. 2013.

[3] C. Ding, Y. Liu, C. Ma, and L. Zeng, "The weight distributions of the duals of cyclic codes with two zeros," *IEEE Trans. Inform. Theory,* vol. 57, no. 12, pp. 8000–8006, Dec. 2011.

[4] K. Feng and J. Luo, "Weight distribution of some reducible cyclic codes," *Finite Fields Appl.*, vol. 14, no. 4, pp. 390–409, Apr. 2008.

[5] T. Feng, "On cyclic codes of length $2^{2^r}-1$ with two zeros whose dual codes have three weights," *Des. Codes Cryptogr.*, vol. 62, pp. 253–258, 2012.

[6] A. Klapper, "Cross-correlations of quadratic form sequences in odd characteristic," *Des. Codes Cryptogr.*,, vol. 3, no. 4, pp. 289–305, June 1997.

[7] T. Kløve, *Codes for Error Detection*, World Scientific, 2007.

[8] S. X. Li, S. H. Hu, T. Feng, and G. Ge, "The weight distribution of a class of cyclic codes related to Hermitian for Graphs," arXiv:1212.6371, 2012.

[9] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics, Vol. 20, Cambridge University Press, Cambridge, 1983.

[10] J. Luo and K. Feng, "On the weight distribution of two classes of cyclic codes," *IEEE Trans. Inform. Theory,* vol. 54, no. 12, pp. 5332–5344, Dec. 2008.

[11] J. Luo and K. Feng, "Cyclic codes and sequences from generalized Coulter-Matthews function," *IEEE Trans. Inform. Theory,* vol. 54, no. 12, pp. 5345–5353, Dec. 2008.

[12] C. Ma, L. Zeng, Y. Liu, D. Feng, and C. Ding, "The weight enumerator of a class of cyclic codes," *IEEE Trans. Inform. Theory,* vol. 57, no. 1, pp. 397–402, Jan. 2011.

[13] X. H. Tang, P. Udaya, P. Z. Fan, "A new family of nonbinary sequences with three-level correlation property and large linear span," *IEEE Trans. Inform. Theory,* vol. 51, pp. 2906–2914, Aug. 2005.

[14] H. M. Trachtenberg, *On the crosscorrelation functions of maximal linear recurring sequences*, Ph.D. dissertation, Univ. South. Calif., Los Angels, 1970.

[15] B. Wang, C. Tang, Y. Qi, Y. X. Yang, and M. Xu, "The weight distributions of cyclic codes and elliptic curves," *IEEE Trans. Inform. Theory,* vol. 58, no. 12, pp. 7253–7259, Dec. 2012.

[16] M. Xiong, "The weight distributions of a class of cyclic codes," *Finite Fields Appl.*, vol. 18, no. 5, pp. 933–945, Sep. 2012.

[17] J. Yuan, C. Carlet and C. Ding, "The weight distribution of a class of linear codes from perfect nonlinear functions," *IEEE Trans. Inform. Theory,* vol. 52, no. 2, pp. 712–717, Feb. 2006.

[18] X. Zeng, L. Hu, W. Jiang, Q. Yue and X. Cao, "Weight distribution of a p-ary cyclic code," *Finite Fields Appl.*, vol. 16, no. 1, pp. 56–73, Jan. 2010.